Bộ môn An toàn Thông tin – Khoa Mạng máy tính và Truyền thông
Trường Đại học Công nghệ Thông tin – Đại học Quốc gia thành phố Hồ Chí Minh

1

Lab

ÔN TẬP KIẾN THỨC CƠ BẢN

Ứng dụng web

(HTML, Javascript, PHP, CSDL)

Thực hành môn Bảo mật web và ứng dụng

Tháng 3/2021

Lưu hành nội bộ

<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

Mọi góp ý về tài liệu, vui lòng gửi về email inseclab@uit.edu.vn

BEE SECURE
INSECLAB

A. TỔNG QUAN

1. Mục tiêu

- Ôn tập kiến thức cơ bản về web (các ngôn ngữ HTML, Javascript, PHP…) để chuẩn bị kiến thức cho phần bảo mật.
- Giúp sinh viên có được kiến thức thao tác với JavaScript (như validation, Ajax,…), PHP và Cơ sở dữ liệu.

2. Thời gian thực hành

- Thực hành tại lớp: **5** tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa **13** ngày.

3. Kiến thức nền tảng

LEMP là tên gọi của một nhóm phần mềm được sử dụng để chạy ứng dụng web được viết bằng ngôn ngữ lập trình PHP. Đây là từ viết tắt bao gồm: hệ điều hành Linux, máy chủ web Nginx (Engine-X), dữ liệu backend được lưu trữ tại cơ sở dữ liệu MySQL và các tiến trình được kiểm soát bởi PHP.

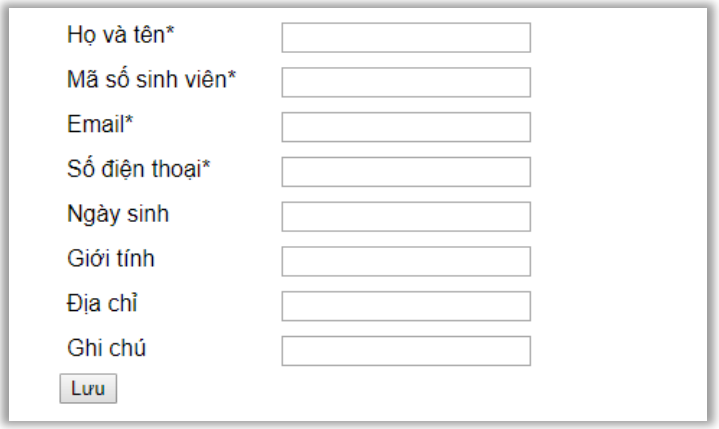
B. CHUẨN BỊ MÔI TRƯỜNG

1. Cài đặt WMware Workstation

Hướng dẫn cài đặt, tạo máy và cấu hình máy ảo trên **WMware Workstation** trong tập tin PDF đính kèm: *HƯỚNG DẪN CÀI ĐẶT MÔI TRƯỜNG MÁY ẢO VỚI VMWARE.*

2. Các tập tin chuẩn bị

- Để thuận tiện cho quá trình thực hành và tập trung vào những phần quan trọng, GVTH cung cấp sẵn cho sinh viên một số tập tin như sau:
    - **SimpleForm.html** tạo một form đơn giản, trong đó bao gồm:
        - Đoạn mã HTML để tạo form đơn giản gồm 8 trường Họ và tên, Mã số sinh viên, Email, Số điện thoại, Ngày sinh, Giới tính, Địa chỉ và Ghi chú.
        - Đoạn mã Javascript bắt sự kiện nhấn nút Lưu của form.
        - Import tập tin jQuery hỗ trợ cho **Error! Reference source not found.**.



Hình 1. Form thông tin mẫu

- **submit_form.php** xử lý yêu cầu submit form được gửi từ **SimpleForm.html**. Tập tin này sẽ thực hiện kết nối đến MySQL server để lưu thông tin.
- **login.php** xử lý yêu cầu đăng nhập và có kết nối với MySQL server, tuy nhiên không có mã nguồn để gọi nó từ tập tin HTML.

- Sinh viên có thể tải image Ubuntu tại http://mirror.bizflycloud.vn/ubuntu-releases/20.04/
- Sinh viên thiết lập cấu hình máy ảo như bảng bên dưới (hoặc có thể thay đổi tùy vào cấu hình của mỗi sinh viên. Tuy nhiên, card mạng vẫn phải giữ nguyên)

Máy ảo	Ubuntu
Dung lượng RAM	2 GB
Vi xử lý	1 Processor, 4 Core
Dung lượng ổ cứng	20 GB
Card mạng	NAT (VMnet8)

3. Triển khai Webserver

a) Cài đặt Webserver Nginx

Nginx là một dạng web server mang lại hiệu suất cao cho việc hiển thị các trang web cho người dùng truy cập.

Cập nhật các gói phần mềm và cài đặt Nginx:

```
sudo apt update

sudo apt install nginx -y
```

Sau khi cài đặt xong, máy chủ web Nginx sẽ hoạt động và chạy trên máy chủ Ubuntu. Nhập địa chỉ ip local hoặc qua lệnh *ifconfig, ip link..* trên trình duyệt, chúng sẽ đưa ta đến trang mặc định của Nginx.

```
http://server_domain_or_IP
```

Nếu nhìn thấy kết quả như hình này có nghĩa là đã cài đặt thành công Nginx.

b) Cài đặt MySQL

MySQL là một hệ quản trị cơ sở dữ liệu phổ biến được sử dụng trong môi trường PHP. Một lần nữa sử dụng apt để cài đặt gói phần mềm.

```
sudo apt install mysql-server -y
```

Sau khi hoàn tất cài đặt, nên thiết lập khuyến nghị bảo mật để loại bỏ các cài đặt mặc định không an toàn.

```
sudo mysql_secure_installation
```

Để tiến hành truy cập MySQL gõ lệnh sau:

```
mysql -u root -p
```

c) Cài đặt PHP

PHP được nhằm mục đích xử lý code và tạo nội dung cho webserver của bạn.

```
sudo apt install php-fpm php-mysql -y
```

d) Dựng Web

Sao chép 2 tập tin được cung cấp vào thư mục tương ứng của web server ở đường dẫn **/var/www/html/.** Truy cập thông qua đường dẫn sau

http://server_domain_or_IP/SimpleForm.html. Điều chỉnh IP theo cấu hình khi cài đặt.

C. THỰC HÀNH

1. HTML và Javascript

a) Hệ thống tập tin Linux

> **Bài thực hành 1:**Điều chỉnh tập tin mã nguồn **SimpleForm.html** để thỏa mãn các yêu cầu bên dưới.

Dùng thuộc tính mặc định của HTML, hiện thực các ràng buộc sau:

- Bắt buộc phải nhập **04** trường **Họ và tên, Mã số sinh viên, Email** và **Số điện thoại** trước khi lưu.
- Trường **Email** cần kiểm tra người dùng có nhập đúng định dạng email không.
- **Số điện thoại** và **Mã số sinh viên** có độ dài tối đa 15 ký tự.

***Gợi ý**: Trường **Email** đổi type khác, tham khảo các thuộc tính của thẻ <input>.*

> **Bài thực hành 2:** Viết mã nguồn **Javascript** (có thể ở trong hoặc ngoài tập tin HTML) thực hiện kiểm tra trường **Họ và tên** chỉ cho nhập chữ và khoảng trắng.

***Gợi ý:** Sinh viên có thể kiểm tra lúc nhấn nút **Submit** hoặc dùng các sự kiện keypress để kiểm tra lúc nhập cho trường **Họ và tên**.*

b) PHP và Cơ sở dữ liệu

> **Bài thực hành 3:** Tạo một bảng trong cơ sở dữ liệu MySQL với các trường tương ứng ở **Bài thực hành 1** thỏa mãn các yêu cầu sau.

- Cơ sở dữ liệu có thể lưu chữ dạng **UTF-8.**
- Các trường tương ứng ở **Bài thực hành 1** 0với **Họ và tên, MSSV, Số điện thoại** và **Email** không được bỏ trống. **Số điện thoại** và **MSSV** có độ dài tối đa 15 ký tự.

> **Bài thực hành 4:** Điều chỉnh mã nguồn trong tập tin **submit_form.php** để nhận các giá trị được submit và lưu vào CSDL dùng MySQL. Điền và submit thử một form để kiểm tra hoạt động của mã nguồn đã điều chỉnh.

Sinh viên có thể lựa chọn 1 trong 3 cách kết nối cơ sở dữ liệu đã được học:

- MySQLi hướng đối tượng
- MySQLi dùng hàm
- PDO

Tham khảo thêm ở đường dẫn:
https://www.w3schools.com/php/php_mysql_connect.asp

***Gợi ý:** Cần đảm bảo:*

- Nút **Lưu** có type là **submit**.

- Đường dẫn xử lý của form đã trỏ đến **submit_form.php**
- Thông tin kết nối CSDL đúng với MySQL đã xây dựng.
- Lấy được các tham số đã nhập trong form và tạo được SQL Command đúng.

c) Tuỳ chỉnh kết hợp giữa form và cơ sở dữ liệu

Bài thực hành 5: Điều chỉnh form và viết mã nguồn Ajax để gửi thông tin form lưu vào CSDL qua Ajax và hiển thị thông báo thành công/thất bại cho người dùng.

Gợi ý: *Cần đảm bảo:*

- Sử dụng nút Lưu mới với type là button.
- Bắt sự kiện click của nút này và xử lý JavaScript với Ajax để gửi form đến URL của submit_form.php.
- Có thể sử dụng jQuery.

Tham khảo thêm ở đường dẫn: https://www.w3schools.com/xml/xml_http.asp hoặc https://api.jquery.com/jquery.ajax/

Bài thực hành 6: Viết một tập tin tương tự khác, trong đó khi mở lên thì tự động gửi một form với các trường tham số như **Bài thực hành 1** đến **submit_form.php**

Gợi ý: *Dùng sự kiện* ***onload*** *của body để submit form tự động. Có thể tự động gửi bằng chức năng input có type "submit" hoặc bằng Ajax.*

d) Vọc một chút

Trong các tập tin được cung cấp, có 1 file **login.php** là file không được gọi từ file HTML, tuy nhiên có thể sử dụng để đăng nhập.

Bài thực hành 7: Phân tích file **login.php**, sinh viên thực hiện các yêu cầu bên dưới.

a. Tạo một bảng chứa thông tin người dùng đơn giản trong MySQL, với các trường phù hợp dựa trên phân tích file login.php.
b. Không sửa mã nguồn HTML trong tập tin SimpleForm.html, hãy sử dụng Javascript để tìm cách tạo một form cho phép nhập tài khoản và gọi tập tin xử lý login.php để đăng nhập

Cần đảm bảo: Thay đổi chỉ có thể tạo ra lúc đang chạy file SimpleForm.html, nội dung của file trên ổ đĩa chỉ cho phép thêm file JavaScript.

Gợi ý: Viết mã nguồn JavaScript thêm form mới hoặc thay nội dung form ở **Bài thực hành 1** bằng một form đăng nhập khi có một sự kiện nào đó (click 1 nút hoặc load trang).

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện **theo nhóm đã đăng ký.**

- Nộp báo cáo kết quả gồm **Code, CSDL được export** và chi tiết những việc (**Report**) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).

  Báo cáo:
- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Đặt tên theo định dạng**: [Mã lớp]-LabX_MSSV1-MSSV2-MSSV3.**

  Ví dụ: [NT213.K11.ANTN.1]-Lab1_1852xxxx-1852yyyy-1852zzzz.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

E. THAM KHẢO

[1] W3Schools – JavaScript, https://www.w3schools.com/js/default.asp
[2] W3Schools – HTML Form Element, https://www.w3schools.com/html/html_forms.asp
[3] W3Schools – PHP, https://www.w3schools.com/php/php_syntax.asp

HẾT

Chúc các bạn hoàn thành tốt!